WHAT IS CLAIMED IS:

Sub a2

1. In an electronic mail (e-mail) system, a method for sending an e-mail message using a secured connection that employs encryption, the method comprising:

receiving at a message transfer agent (MTA) a request from a client for establishing a secured connection with the MTA for sending an e-mail message;

attempting to authenticate the client, through use of a certificate;

if the client cannot be authenticated, terminating the method without establishing the secured connection and without sending the e-mail message;

if the client can be authenticated, establishing the secured connection between the client and the MTA;

determining whether the encryption employed for the secured connection meets a predefined minimum encryption strength;

if the encryption employed does not meet the predefined minimum encryption strength, terminating the secured connection without sending the e-mail message, whereupon the method terminates; and

if the encryption employed does meet the predefined minimum encryption strength, sending the e-mail message.

2. The method of claim 1, wherein said minimum encryption strength comprises a particular key length of a symmetric cipher used for encryption.

3. The method of claim 1, wherein said step of terminating the method without establishing the secured connection includes:

returning a temporary error reply code.

4. The method of claim 1, wherein said step of terminating the method without establishing the secured connection includes:

returning a permanent error reply code.

5. The method of claim 1, wherein the e-mail message is returned to an original sender for the message if the client cannot be authenticated.

6. The method of claim 1, wherein the e-mail message is queued for future sending if the client cannot be authenticated.

7. The method of claim 1, wherein said step of determining whether the encryption employed for the secured connection meets a predefined minimum encryption strength employs SASL (Simple Authentication and Security Layer) protocol.

8. The method of claim 1, wherein said client is remote from said e-mail system.

9. The method of claim 1, wherein said client includes a Mail User Agent.

10. The method of claim 10, wherein the Mail User Agent communicates with the e-mail system via SMTP (Simple Mail Transport Protocol).

11. The method of claim 1, wherein said MTA comprises a Sendmail-compatible Message Transfer Agent (MTA) and wherein said method is controlled, at least in part, by a configuration file for the Sendmail-compatible MTA.

12. The method of claim 1, wherein said certificate comprises a signed public key.

13. The method of claim 1, wherein said certificate comprises an X.509 certificate.

14. The method of claim 1, wherein said step of terminating the method without establishing the secured connection includes:

rejecting at least some subsequent SMTP commands received from the client.

15. The method of claim 14, wherein the rejected SMTP commands are rejected with an error.

16. In an electronic mail (e-mail) system, a method for sending an e-mail message using a secured connection that employs encryption, the method comprising:

attempting at a first message transfer agent (MTA) to establish a secured connection with a second MTA for sending an e-mail message;

attempting to authenticate the second MTA, through use of a certificate;

if the second MTA cannot be authenticated, terminating the method without establishing the secured connection and without sending the e-mail message;

if the second MTA can be authenticated, establishing the secured connection between the first MTA and the second MTA;

determining whether the encryption employed for the secured connection meets a predefined minimum encryption strength;

if the encryption employed does not meet the predefined minimum encryption strength, terminating the secured connection without sending the e-mail message, whereupon the method terminates; and

if the encryption employed does meet the predefined minimum encryption strength, sending the e-mail message.

17. The method of claim 16, wherein said minimum encryption strength comprises a particular key length of a symmetric cipher used for encryption.

18. The method of claim 16, wherein said step of terminating the method without establishing the secured connection includes:

returning a temporary error reply code.

19. The method of claim 16, wherein said step of terminating the method without establishing the secured connection includes:

returning a permanent error reply code.

20. The method of claim 16, wherein the e-mail message is returned to an original sender for the message if the second MTA cannot be authenticated.

21. The method of claim 16, wherein the e-mail message is queued for future sending if the second MTA cannot be authenticated.

22. The method of claim 16, wherein said step of determining whether the encryption employed for the secured connection meets a predefined minimum encryption strength employs SASL (Simple Authentication and Security Layer) protocol.

23. The method of claim 16, wherein said second MTA is remote from said e-mail system.

24. The method of claim 16, wherein said first MTA originally received the e-mail message from a client that connects to the e-mail system using a Mail User Agent.

25. The method of claim 24, wherein the Mail User Agent communicates with the e-mail system via SMTP (Simple Mail Transport Protocol).

26. The method of claim 16, wherein said first MTA comprises a Sendmail-compatible Message Transfer Agent (MTA) and wherein said method is controlled, at least in part, by a configuration file for the Sendmail-compatible MTA.

27. The method of claim 16, wherein said certificate comprises a signed public key.

28. The method of claim 16, wherein said certificate comprises an X.509 certificate.

29. The method of claim 16, wherein the first MTA communicates with the second MTA using SMTP (Simple Mail Transport Protocol).

30. The method of claim 29, wherein said step of terminating the method without establishing the secured connection includes:

issuing an SMTP QUIT command.

31. An electronic mail (e-mail) system comprising:

a message transfer agent (MTA) available for a client to connect to;

program logic for authenticating the client, through use of a certificate;

program logic for establishing a secured connection between the client and the MTA in instances where the client can be authenticated;

program logic for testing encryption strength of the secured connection; and

program logic for terminating the secured connection in instances where the secured connection has inadequate encryption strength.

32. The system of claim 31, wherein the client includes Mail User Agent (MUA) software.

33. The system of claim 31, wherein the e-mail message is communicated to the MTA via SMTP (Simple Mail Transport Protocol).

34. The system of claim 31, wherein said certificate comprises a signed public key.

35. The system of claim 31, wherein said certificate comprises an X.509 certificate.